Vragen? Opmerkingen? Tips?
Mail ze naar
brieven@clickx.be.

DOE HET ZELF

BRIEVEN

WORKSHOPS

WORKSHOPREEKS WEB 2.0

HINTS&TIPS

CURSUS

VERGEET DE GIDS NIET

Brief van de week

De Clickx-redactie wordt elke dag overstelpt met vragen van lezers. Sommige problemen zijn te specifiek om in het magazine te behandelen, maar andere vragen zijn dan weer zo interessant dat ze meer verdienen dan een kort antwoordje. Daarom selecteren we voor elke Clickx Magazine een vraag van een lezer, die we dan uitwerken in een complete workshop. De vraag vind je op deze pagina, de workshop staat op de volgende twee pagina's. Veel plezier!

BLAUW GEËRGERD?



Bij het opstarten van Windows XP krijg ik telkens een blauw scherm te zien, met daarop de melding 'IRQL_NOT_LESS_OR_EQUAL'. **Wat is er aan de hand?**

ALBERT MERTENS



Een blauw scherm, soms smalend ook wel een *blue screen of death* (BSOD) genoemd, duikt op wanneer Windows op een probleemsituatie botst, waardoor een betrouwbare werking niet langer mogelijk is. Het is dan een kwestie van de oorzaak van die 'stopfout' te achterhalen, en dat is precies wat we in deze workshop gaan doen...





BLAUW GEËRGERD?



WAT DOEN WE?

- NAGAAN WAT DE OORZAAK VAN (EN DE OPLOSSING VOOR) EEN 'BLUE SCREEN' IS.

WAARMEE?

- FUNCTIES EN TOOLS BINNEN WINDOWS ZELF (MET WAT HULP VAN HET WEB)

HOELANG?

- VAN 15 MINUTEN TOT 1 UUR (AFHANKELIJK VAN DE FOUTMELDING)

MOEILIJKHEID?



Het precieze moment waarop zo'n stopfout verschijnt, zegt vaak al iets over de mogelijke oorzaak. Duikt zo'n fout op bij het opstarten van Windows (gewoonlijk net voor de grafische interface geladen wordt), dan houdt dit meestal verband met corrupte systeembestanden of met incompatibele stuurprogramma's of services. Stopfouten kunnen echter ook voorkomen tijdens het werken met de pc, en dan vooral wanneer Windows op ernstige software- of hardwarefouten botst. Stopfouten die schijnbaar willekeurig opduiken, hebben vaak te maken met gebrekkig systeemgeheugen, een oververhitte processor of een onbetrouwbare harde schijf.
Er zijn dus tal van oorzaken mogelijk, en uitvissen wat nu de echte boosdoener is, is dan ook de belangrijkste stap naar het zoeken van een oplossing. De verschillende stappen zijn gerangschikt per moeilijkheid, waarbij stap 4 en stap 5 voor gevorderden zijn. Waag je hier dus alleen maar aan, als je zeker weet wat je aan het doen bent!

STAP 1 / INSTELLINGEN

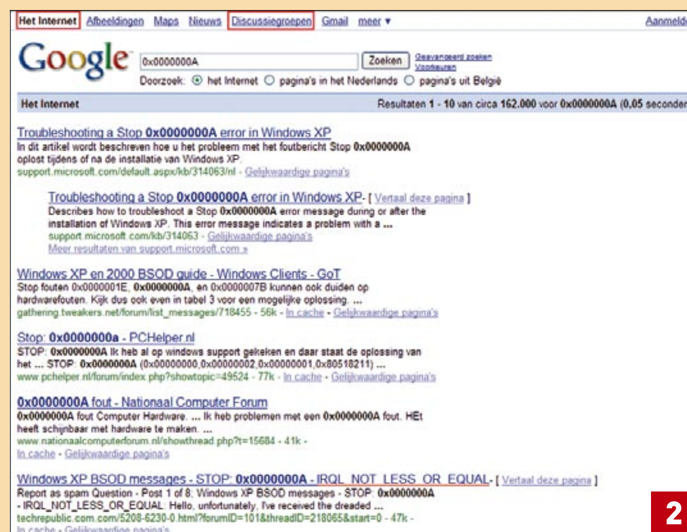
Zelfs wie op een gezond systeem kan bogen, doet er goed aan Windows zo in te stellen dat zo'n stopfout bij rampspoed tenminste lang genoeg in beeld blijft om de melding te kunnen lezen en noteren. Klik daarom met de rechtermuisknop op (**Deze**) **computer** en kies **Eigenschappen**. Open het tabblad **Geavanceerd** en druk op de onderste knop **Instellingen**. Verwijder zonodig het vinkje bij **De computer automatisch opnieuw opstarten** (zie afbeelding 1). Zorg wel dat er een vinkje staat bij **Een gebeurtenis in het systeemlogboek vastleggen** (zie stap 3). Kies bij **Foutopsporingsgegevens vastleggen** bij voorkeur **Dump van kernelgeheugen**, noteer het pad bij **Dumpbestand** en plaats een vinkje bij **Bestaand bestand overschrijven** (zie ook stap 4). Bevestig met **OK**.



Zorg voor optimale instellingen, ingeval dát...

STAP 2 / BUGCHECK CODE

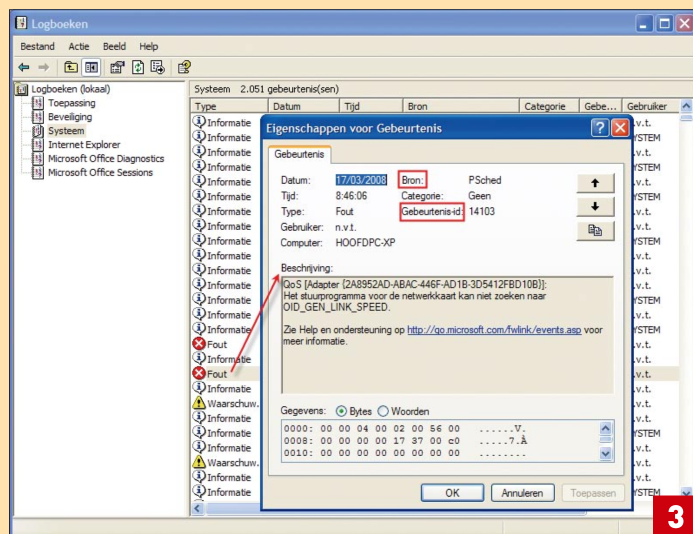
Het ergste is gebeurd: je krijgt een BSOD op je neus! Alvast niet panikeren, en pen en papier bij de hand nemen. Het blauwe scherm bevat met wat geluk namelijk waardevolle informatie die je op het spoor van de dader kan zetten. Vast ingrediënt in zo'n foutbericht is de zogenoemde *bugcheck code*: een hexadecimaal stopfoutnummer dat het fouttype aangeeft, gevolgd door (vier) parameters, eveneens in hexadecimaal formaat. Noteer de bugcheck code (bijvoorbeeld 0x000000ED) en voer die in in een zoekmachine als Google (zie afbeelding 2). Probeer zeker ook de link **Discussiegroepen** uit: heel vaak bots je dan op andere gebruikers die met dezelfde problemen te kampen hadden. Als het meezit, toont het BSOD-scherm je zelfs informatie over een of andere driver: mogelijk – maar niet zeker – ligt dit stuurprogramma dan aan de basis van de stopfout (zie ook kaderstukje).



De bugcheck code: cryptisch, maar vaak erg informatief.

STAP 3 / LOGBOEKEN

Heeft de bugcheck code je geen bruikbare tips opgeleverd? Dan kan je nog aankloppen bij de logboeken die Windows zelf bijhoudt. Tik hiervoor de opdracht *eventvwr.msc* (*event viewer*) in bij **Start** (of in Vista bij **Zoekopdracht starten**) en bevestig met **Enter**. Er duikt nu een dialoogvenster op, waar in het linkerpaneel de verschillende logboeken staan opgelijnd. De kans is groot dat de stopfout in het logboek **Systeem** geregistreerd staat. Dubbelklik dus allereerst op dit logboek, zodat de inhoud in het rechterpaneel te voorschijn komt. Ga nu vooral op zoek naar fouten in de kolom **Type** (door de kolomtitel aan te klikken kan je hier zelfs op sorteren). Concentreer je op fouten die rond hetzelfde tijdstip zijn opgedoken als de BSOD. Dubbelklik vervolgens op zo'n foutmelding. Je krijgt nu het eigenschappenvenster voor die gebeurtenis te zien (zie afbeelding 3). Misschien zetten de beschrijving en de bijhorende link je al in de juiste richting, maar die kans is eerder klein. Je doet er wellicht beter aan te noteren wat er bij **Bron** en bij **Gebeurtenis-ID** vermeld staat. Gewapend met deze informatie surf je nu naar (een van) de volgende sites: http://eventid.net en www.microsoft.com/technet/support/ee/ee_advanced.aspx. Mogelijk leveren deze sites wél vol-



De logboeken van Windows: ijverige notulanten!

doende informatie op om de dader te ontmaskeren. Bij de tweede site kan je **Dutch** selecteren, maar de Engelstalige databank blijkt wel een heel stuk uitgebreider.

STAP 4 / DEBUGGER (1)

Nog altijd geen oplossing in zicht? Dan kan je het ofwel met een paar 'universele' ingrepen proberen (zie kaderstukje), ofwel meer gesofisticeerd geschut bovenhalen – voor gevorderden, dus. Dat vind je in de vorm van een zogenoemde debugger: een tool voor het opsporen van fouten. Je kan er een downloaden op www.microsoft.com/whdc/devtools/debugging (**Install Debugging Tools for Windows 32-bit Version**, versie 6.8.4.0). Na de – overigens erg eenvoudige – installatie van deze tool ga je met de Verkenner naar het installatiepad en start je windbg.exe op. Open

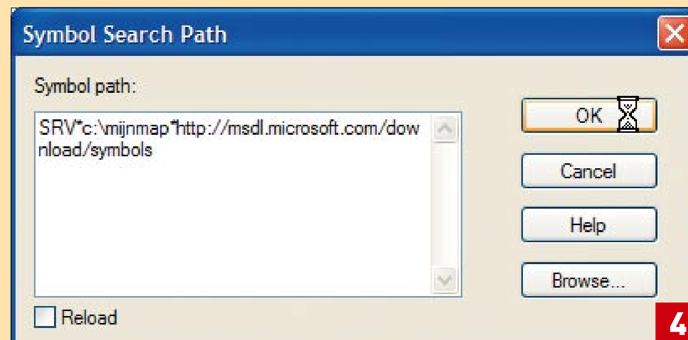
HERSTELOPERATIES

Kom je met geen stokken de exacte oorzaak van het BSOD te weten, dan kan je altijd nog (een van) de volgende procedures proberen.

1. Start Windows in veilige modus op door na het inschakelen van de pc even de **F8**-toets ingedrukt te houden. Start van hieruit het Windows Systeemherstel op (**Alle programma's, Bureau-accessoires, Systeemwerkset**) en kies een herstelpunt kort voordat de stopfout de eerste keer opdook. Hou er wel rekening mee dat soft- of hardware die je eventueel nog ná die datum geïnstalleerd hebt, wellicht niet meer correct zal functioneren.

2. Zijn de problemen begonnen na de installatie van een stukje hardware of na de update van een stuurprogramma, dan is een andere driver of het terugrollen naar de vorige versie een mogelijke oplossing. Klik hiervoor met de rechtermuisknop op **Deze computer** en kies **Eigenschappen**. Ga naar het tabblad **Hardware** en druk op de knop **Apparaatbeheer**. Klik met de rechtermuisknop op het bewuste apparaat en selecteer **Eigenschappen**. Open het tabblad **Stuurprogramma** en kies **Stuurprogramma bijwerken** dan wel **Vorig stuurprogramma**. Volg de verdere instructies op het scherm.

3. Helpt dat allemaal niet, herstart de pc dan nog een keer en selecteer vanuit het opstartmenu (via de toets **F8**) de optie **Laatst bekende juiste configuratie**. Windows zal dan trachten op te starten met de systeeminstellingen van de meest recente sessie die succesvol was opgestart.

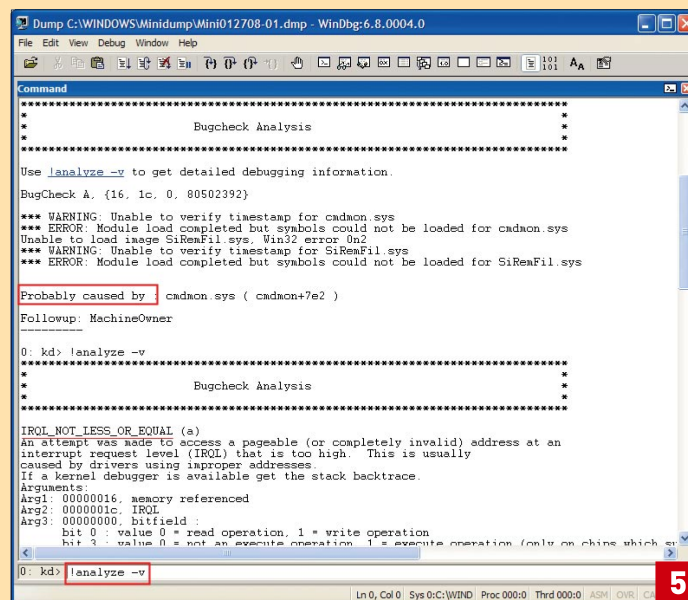


Haal de nodige symbolen op uit een online databank.

vervolgens het menu **File**, selecteer **Symbol File Path** en vul het volgende pad in: SRV*c:\mijnmap*http://msdl.microsoft.com/download/symbols (waarbij je c:\mijnmap vervangt door het pad naar een eigen, nieuw gecreëerde map) (zie afbeelding 4). Bevestig met **OK**. Open alweer het **File**-menu en kies dit keer **Open Crash Dump**, waarna je naar het juiste dumpbestand bladert (zie stap 1). Zorg wel dat je firewall de tool de doorgang naar het internet niet belemmert.

STAP 5 / DEBUGGER (2)

Na het inladen van de symbolenbibliotheek – een proces dat wel even kan duren – krijg je dan allerlei gegevens te zien in het Command-venster. Vooral de informatie bij de Bugcheck Analysis kan je op het goede spoor zetten. Heel vaak lees je achter *Probably caused by* de juiste oorzaak van de crash (zie afbeelding 5). In ons voorbeeld zou cmdmon.sys er vermoedelijk voor iets tussen zitten. Nog meer gedetailleerde informatie kan je opvragen door op de commandoregel, helemaal onderaan het venster, de volgende instructie in te tikken achter kd>: !analyze –v. Tik hier ook even de opdracht .hh in, gevolgd door de symbolische foutnaam die je te zien kreeg in het BSOD (bijvoorbeeld .hh irql_not_less_or_equal of .hh unmountable_boot_volume). Je belandt dan in een extra hulpscherm van de tool waarin je onder meer uitleg krijgt over de precieze betekenis van de hexadecimale parameters van de bugcheck code (zie ook stap 2). Succes! ♦



Veel gedetailleerder krijg je het niet!